## REMARKS

This Amendment and Request for Reconsideration is filed in response to the Office Action of September 27, 2006 in which claims 1-12 were rejected. Claims 13-18 have been added and are directed to circuitry very similar to that claimed in claims 1-6 except not using means-plus-function language and are intentionally not invoking 35 USC 112, sixth paragraph.

The rejections of the Office Action pertain to novelty in view of *Moscovici* (U.S. 6,678,765) and obviousness in view of *Moscovici* taken together with *Smith* (U.S. 6,449,281).

In applicants' opinion no claim is anticipated by *Moscovici*, and no claim is obvious in the light of the combination of *Moscovici* and *Smith.*

Closest Prior Art

*Moscovici* generally discloses, for example with reference to column 3, lines 14-28, an embedded system having a general purpose CPU and a DSP, where both processors are adapted to perform tasks associated with the transmission and reception of information. However, the CPU is adapted to perform code consuming tasks while the DSP is adapted to perform tasks that require less program code. Hence, the DSP handles digital signal processing tasks and the CPU handles mainly control tasks. During most of the time the CPU can handle tasks that are not related to the transmission and reception of data, such as browsing or controlling a screen of a mobile phone/browser, while the DSP which does not have to execute lengthy programs in relatively very short periods can be driven by a slower clock.

An object of the system set forth in *Moscovici* is to provide an improved modem, which is relatively cost effective and fast. The distribution of tasks between the DSP and the CPU enables, as is mentioned in column 3, lines 29-35, the CPU to handle one part of a modem handshaking process while the DSP can handle another part of the process and the exchange of information that follows a successful handshaking process.

Clearly, the technical effect of the system described in *Moscovici* is that data processing can be undertaken in a more efficient manner by distributing data processing and control tasks between a DSP and a CPU.

The Invention

The present invention as defined by the independent claims is based on the idea that circuitry is provided in which a processor is operable in at least two different modes, one first secure operating mode and one second unsecure operating mode. In the secure mode, the processor has access to security related data located in various memories located within the circuitry. The security data include cryptographical keys and algorithms, software for booting the circuitry, secret data such as random numbers used as cryptographical key material, application programs etc. The access to these security data and the processing of them need to be restricted, since an intruder with access to security data could manipulate a device, for example a mobile terminal, in which the circuitry of the present invention is implemented. When testing and/or debugging the terminal, access to the security data is not allowed. For this reason, the processor is set in the insecure operating mode, in which mode it is no longer given access to the security data.

The present invention advantageously enables the processor of the circuitry to execute non-verified software downloaded into the circuitry. This allows testing, debugging and servicing of the electronic device and its software without risking that a third party is given access to information which makes it possible to manipulate the security related components of the device so as to affect the security functions when in the secure environment.

Novelty and Non-obviousness

Turning again to *Moscovici* and the novelty rejection of claims 1-4, 6-10 and 12 set forth in the Office Action under items 3-8, it is clear that the *Moscovici* reference does not disclose a storage area where protected data relating to circuitry security is located.

Regarding the Examiner's reference to column 3, lines 40-56; this section discloses memory modules 34, 37 storing CPU control programs such as an operating system, ring detection programs, error calculation programs, etc. Further, the memory modules stores DSP programs such as phase modulator programs, adaptive filter programs, echo cancellers, etc. The programs mentioned in column 3 are clearly not security related. As has been mentioned above, security data may e.g. comprise cryptographical keys and algorithms, software for booting the circuitry, secret data such as random numbers used as cryptographical key material, etc. Further, nowhere in *Moscovici* it is mentioned that the memory modules have a designated storage area for storing protected data relating to circuitry security. In contrast, the CPU has access to a CPU portion 41 of external memory module 34 while the DSP has access to a DSP portion. The CPU does not access the DSP portion and the DSP does not access the CPU portion. Hence, there is no single storage area in which security related data is stored, and to which area a processor has access in one mode and is denied access in another mode.

Regarding the Examiner's reference to column 4, lines 22-35; it is described that data to be transmitted *first* is processed by the CPU and *then* processed by the DSP. This section clearly does not disclose "storage circuit access control means arranged to enable said processor to access said storage area in which said protected data is located when a first processor operating mode is set." The Examiner indicates that this particular section of *Moscovici* discloses that the CPU is enabled to access protected data. However, the data processed by the CPU is subsequently processed by the DSP.

Regarding the Examiner's reference to column 6, lines 3-22; it is described that the CPU instructs the DSP which set of instructions to execute, which is standard procedure in a system like the one disclosed in *Moscovici*. While the DSP is executing the set of instructions, the CPU can perform some other processing. When the DSP has finished the execution, it sends the CPU an END signal. The CPU can thus decide whether to send further instructions to the DSP for execution. Hence, this is just a matter of having a CPU instruct a DSP which code to execute, and has got nothing to do with the feature of the present invention to "prevent a processor from accessing a storage area in which protected data are located when a second processor operating mode is set, thereby enabling the processor to execute non-verified software downloaded into the circuitry". To have two processors taking turns at accessing a buffer (one processor writing the buffer and the other processor reading it) where general purpose code is stored is not the same as preventing a processor from accessing a storage area where protected data is located.

Withdrawal of the novelty rejection of claims 1-4, 6-10 and 12 is requested.

In light of the above, regarding the obviousness rejection of dependent claims 5 and 11, *Smith* does not add any substantial matter that can compensate for the lacking features of *Moscivici*, and therefore the claims rejected on this ground are patentable for at least the same reasons advanced above in overcoming the novelty rejection and withdrawal of the obviousness rejection of dependent claims 5 and 11 is requested as well.

Conclusion

As can be deduced from the above argumentation, there are many differences between the present invention and the system set forth in *Moscovici*. It is applicants' position that the present invention discloses a rather different type of system than the system disclosed in

*Moscovici*. Further, the present invention has a completely different object and a different technical effect. For these reasons, applicant believes the present invention is novel as well as non-obvious over the applied prior art and withdrawal of the Section 102 and 103 rejections thereof is requested.

It is believed that no fees are due on account of this amendment but if this is incorrect the Director is authorized to deduct the required fee from our deposit account 23-0442. This includes us possibly overlooking any needed petition for extension of time and fee that may be due.

The objections and rejections of the office action of September 27, 2006, having been obviated by amendment or shown to be inapplicable, withdrawal thereof is requested and passage of claims 1-19 to issue at an early date is earnestly solicited.

Respectfully submitted,

Francis J. Maguire
Attorney for the Applicant
Registration No. 31,391

FJM/mo
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, Connecticut 06468
(203) 261-1234